Filter on TCP Expert Information Elements

Apply a display filter for **tcp.analysis.flags** to show packets that match the Expert Info Notes and Warnings triggers.

Figure 178 shows the result of applying a tcp.analysis.flags display filter to an entire trace file. This is a fast method to detect TCP-based problems in a trace file.

Use a tcp.analysis.flags Filter Expression Button

Consider creating and saving this display filter as a filter expression button called **Bad TCP**. To be most accurate, add && !tcp.analysis.window_update to the filter. When you open trace files, click your new Bad TCP Filter Expression button to locate the most common TCP-related network problems.Expert Infos window

You can create a display filter to examine packets that meet a specific Expert Info severity level. The following provides examples of the four severity level filters ("Details" and "Packet Comments" are not considered a severity levels):

```
expert.severity==error
expert.severity==warn
expert.severity==note
expert.severity==chat
```

Another display filter is available for packets that are part of a specific Expert Info group. The syntax is expert.group==<group>. Some of the Wireshark Expert Info groups are:

- Checksum—a checksum was invalid
- Sequence—sequence number was not correct or indicated a retransmission
- Malformed—malformed packet or dissector bug
- Protocol—invalid field value (possible violation of specification)

M http-iewithtoolbar.pcapng															
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatistics	Telephor	n <u>y T</u> ools	Interna	ls <u>H</u> elp					
		1 61	in.	la r	×2	8 Q	\$ \$	- - 	₽ [⊕, ⊖,	11			* 0
Filter	Filter: tcp.analysis.flags && !tcp.analysis.window_update Expression Clear Apply Save														
No.	Time			Source			Destinatio	n		Protocol	Length	Info			
145	32	. 417	665	205.2	234.17	5.175	24.6.	173.22	0	HTTP	1514	[TCP	Prev	ious	segmen [.]
146	32	.417	696	24.6.	173.2	20	205.2	34.175	.175	TCP	66	[TCP	Dup A	ACK [144#1] (
147	32	.418	471	205.2	234.17	5.175	24.6.	173.22	0	HTTP	1514	[TCP	Out-0)f-01	rder] Co
238	32	. 492	576	205.2	234.17	5.175	24.6.	173.22	0	HTTP	599	[TCP	Prev	ious	segmen [.]
239	32	. 492	670	24.6.	173.2	20	205.2	34.175	.175	TCP	66	[TCP	Dup /	ACK 2	237#1] (
240	32	. 494	231	205.2	234.17	5.175	24.6.	173.22	0	HTTP	1514	[TCP	Out-()f-01	rder] Co
	4 .	5				Same.	~	-		-		-			Marthan - chi

Figure 178. A display filter shows TCP problems [http-iewithtoolbar.pcapng]